Notice of Allowability	Application No.	Applicant(s)	
	09/850,239	LEE ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed 7-24-06*.

2. ☒ The allowed claim(s) is/are *2,4-19,21-25,28-57 and 66-77*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

1. Claims 2, 4-19, 21-25, 28-57, and 66-77 are pending in this application and have been examined.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Diane Dunn-McKay, Esq., on 9-11-06.

IN THE SPECIFICATION

Lines 8 and 9 on page 2 of the Specification are now amended as follows:

Advanced Encryption Standard (AES)"[[.]]~~, http://csrc.nist.gov/encryption/aes/pre-round1/aes9709.html,~~ Since conventional microprocessors are word-oriented, performing

IN THE ABSTRACT

The Abstract is stricken and replaced with the following version:

The present invention provides permutation instructions usable in a programmable processor for solving permutation problems in cryptography, multimedia and other applications. PPERM and PPERM3R instructions are defined to perform permutations by a sequence of instructions with each sequence specifying the position in the source for each bit in the destination. In the PPERM instruction bits in the destination register that change are updated and bits in the destination register that do not change are set to zero. In the PPERM3R instruction bits in the destination register that change are updated and bits in the destination register that do not change are copied from intermediate result of previous PPERM3R instructions. Both PPERM and PPERM3R instructions can individually do permutation with bit repetition. Both PPERM and PPERM3R instructions can individually do permutation of bits stored in more than one register. In an alternate embodiment, a GRP instruction is defined to perform permutations.

IN THE CLAIMS

Section d. of claim 77 is replaced with the following:

d. repeating steps a. through c. for different groups of bits in said destination register, wherein after a final permutation instruction a desired permutation of said source register is determined and said determined permutation instructions form a permutation instruction sequence: and

Allowable Subject Matter

3. Claims 2, 4-19, 21-25, 28-57, and 66-77 are allowed.

4. The following is an examiner's statement of reasons for allowance:

The closest prior art in the field: Cole US 6,865,272, and Turkowski US 5,524,256, do not teach the combination of features of the claimed invention as set forth in the independent claims, particularly including:

As per claims 4, 6, and 21, a method, and a system for performing an arbitrary permutation in a programmable processor including; performing the permutation based on a permutation instruction that is defined by: a first parameter indicating which k bits in a destination will change, a reference to the source register which contains the source sequence of bits to be permuted, a reference to a configuration register which contains configuration bits for indicating which said bits in the source register are assembled, and a reference to the destination register.

As for claim 5, a method of performing an arbitrary permutation in a programmable processor including: wherein after a final permutation instruction, a desired permutation of a source register is determined and used to determine a permutation instruction for source bits in a source register, and where the permutation

instruction forms a sequence where each of *k* bits in a final permutation is determined by l*gn* bits in a destination register that specify which bits in a source register to change.

As for claim 8: a method of performing an arbitrary permutation in a programmable processor including; determining an intermediate sequence of bits that a final arrangement is transformed from, and determining a permutation instruction for transforming the intermediate sequence into the final sequence by dividing the intermediate sequence into a first group and a second group, combining the groups, and subsequently repeating the steps using the determined intermediate sequence of bits from the first step as said final arrangement of bits in the second step until an intermediate sequence of bits is obtained that is the same as the source sequence of bits, wherein the determined permutation instructions, in reversed order, form a permutation instruction sequence.

As for claims 14 and 32: a method and a system for performing an arbitrary permutation in a programmable processor including; determining a final arrangement of a sequence of bits to be permuted and determining a number of monotonically increasing sequences (MIS) in the arrangement, determining a first group of MIS's and a second group of MIS's and combining each element of the first group sequentially with each element of the second group.

As for claims 17 and 35: a method and a system for performing an arbitrary permutation in a programmable processor including the use of GRP permutation instructions in permuting bits from a source register.

As for claim 28, a system for performing an arbitrary permutation in a programmable processor including: where a permutation instruction comprises a reference to a source register which contains an arrangement of a source sequence of bits, a reference to a configuration register which contains configuration bits, and a reference to a destination register to which an intermediate sequence of bits is placed; wherein a series of determined permutation instructions form a permutation instruction sequence, and bits in the source arrangement are divided into said first group if a configuration bit is 0 and into said second group if a configuration bit is 1.

As for claims 38, 46, 48, and 50: a method of performing an arbitrary permutation in a programmable processor including use of a PPERM permutation instructions in permuting bits from a source register. The inclusion of a reference to a PPERM instruction in claim 38 makes the phrase: "for a group of bits in a destination register" clear in context and hence no rejection under 35 USC 112 2nd is warranted.

As for claims 42, 52, 54, and 56: a method, a system, and a computer program embodied in a memory medium that, when read out, cause a processor to undertake steps for performing an arbitrary permutation in a programmable processor including:

use of a PPERM3R permutation instruction in permuting bits from a source register. (The inclusion of a reference to a PPERM3R instruction in claim 42 makes the phrase: "for a group of bits in a destination register" clear in context and hence no rejection under 35 USC 112 2nd is warranted).

As for claim 66: a method of performing an arbitrary permutation including a step wherein after a final permutation instruction, a desired permutation of a source register is determined and the determined permutation instructions form a permutation instruction sequence.

As for claim 76, a method of performing an arbitrary permutation in a programmable processor including the steps of: defining bit positions in a source sequence of bits to be permuted in a source register, determining a permutation instruction with said bit positions to assemble bits from said source sequence of bits, performing said permutation instruction for inserting said assembled bits into a destination register as determined by said bit positions; and repeating the steps for different groups of bits in said destination register, wherein after a final permutation instruction a desired permutation of said source register is determined and said determined permutation instructions form a permutation instruction sequence, and where said permutation has bit repetitions.

As for claim 77, a method of performing an arbitrary permutation in a programmable processor including the steps of: determining a permutation instruction using the bit positions of bits in a sequence to be permuted in a source register, performing said permutation instruction by inserting the source bits into a destination register as determined by the source bit positions, repeating the steps for different groups of bits in the destination register, wherein, after a final permutation instruction, a desired permutation of the source register is determined and the determined permutation instructions form a permutation instruction sequence, and executing at least one other instruction interspersed with said determined permutation instructions during execution of the permutation instruction sequence.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent document teaches a system of permuting a source sequence of bits which is pertinent to the Applicant's disclosure:

Clark 5,734,721

The following non-Patent literature document contains material related to GRP, PPERM, and PPERM3R permutation instructions and is therefore pertinent to the Applicant's disclosure:

Zhijie Shi, Ruby B. Lee: "Bit Permutation Instructions for Accelerating Software Cryptography", in Proc. IEEE Intl. Conf. Application-Specific Systems, Architectures and Processors, pp 138-148, July 2000.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Paul Callahan
PEC

9-8-06